ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

THE NOTORIOUS NINE: TOP CLOUD COMPUTING SECURITY CHALLENGES IN 2017

Abdul Majid Farooqi
School of Engineering Sciences and Technology (SEST)
Jamia Hamdard, Hamdard University
New Delhi, India

Tabrez Nafis
School of Engineering Sciences and Technology (SEST)
Jamia Hamdard, Hamdard University
New Delhi, India

Kafiyah Usvub
School of Engineering Sciences and Technology (SEST)
Jamia Hamdard, Hamdard University
New Delhi, India

Abstract:Unlimited storage, virtual hardware, a vast amount of computing power, low cost, location-independent data access. These are some unique features that are provided by the cloud computing, despite all these great benefits cloud computing facing criticism from the experts regarding its security, many organizations want to move their sensitive and confidential data to the cloud, but still in 2017 they are confused, they are expending lots of money to buy expensive hardware and software for their organization, rather than they buy a cloud storage or cloud computing power at very cheap price. So, what's the reason behind it? Why are they feeling fear to involve in cloud technologies? In this paper, we will try to find out the answers to these questions and will discuss some top cloud security challenges that are currently cloud industry is facing.

Keywords:Cloud Computing, Cloud Security, Cloud Security Challenges.

I. INTRODUCTION

As cloud computing becoming more popular day by day across the globe due to its tremendous features like resource pooling and elasticity, self-service, and on-demand services, pricing, quality of service, unlimited storage, ultimate computing power, location independence, anywhere access, virtualizationetc. it creates more security issues and challenges to the experts, many people are accepting cloud computing and its services for their businesses and transferring all their personal and professional data to the cloud for easy access, but one fear always remain in their hearts, one scary question always confuses their minds. How much their data is secured in the cloud? Are they 100% protected?

In the beginning of cloud computing,it couldn't gain that much popularity and acceptance among people due to its security issues and challenges, with passing years cloud technologies emerged rapidly and it is ruling the world now.Cloud Security Alliance (CSA) found that more than 70% of the world's business occupied by cloud computing [1]. Although acceptance of cloud computing has become more common, security challenges still exist.

Here in this paper,we will discuss cloud computing and its type and service models, also, we will discuss top cloud computing security threats in 2017 called "The Notorious Nine". Our paper is structured as follows: InSection 2 we will discuss related research or related work and will talk what other people have done in their paper related to cloud security and challenges. Section 3 is based on an overview of cloud computing, in this section, we will discuss cloud and cloud computing definition, types of cloud and cloud service models. Section 4 will be based on security challenges in cloud computing, in this section, we will discuss top nine security issues of cloud computing called The Notorious Nine. In section 5 we will conclude our paper.

II. RELATED WORK

Priya Anand [2] gives security challenges of cloud computing, she has also suggested a pattern-based security framework for cloud computing and defined the characteristics of the security pattern system.

Napoleon C. Paxton [1] talks about three major security challenges of cloud computing: 1. Data Breaches, 2. The Hijacking of account, 3. Multitenancy. He also purposed a solution to these threats.

Khalid EI Makkaoui [19] proposed a new cloud security and privacy model into layers that can help cloud providers to identify and classify different cloud security and privacy issues, to make the difference between various sources of cloud threats, and to adopt necessary countermeasures in order to build confidence in cloud services and also to provide secure services. Also, he presented in his paper some security threats and attacks and proposed some countermeasures.

Rabi Prasad Padhy [20] discussed various models of cloud computing, security issues and research challenges in cloud computing.

III. OVERVIEW OF CLOUD COMPUTING

The word cloud represents as the internet or inter-connected computer systems or simply a giant network system. Cloud (Data Centers) exists at certain remote locations mostly hidden from the user, the user doesn't know where his data is saved. It is providing many services over the internet or over the network, such as public networks and private networks, for

example, Local Area Network (LAN), Wide Area Network (WAN) or even Virtual Private Network (VPN). Web Conferencing, Customer Relationship Management (CRM), Email etc. are the applications of Cloud, etc. [3].

Now the Cloud Computing In simple words is the name of delivering computing services over the cloud or the internet. The computing services describe as networking, servers, databases, storage, software, applications, hardware, infrastructure and more. Cloud providers who provide these services over the internet charge for their services as per usage basis [4].

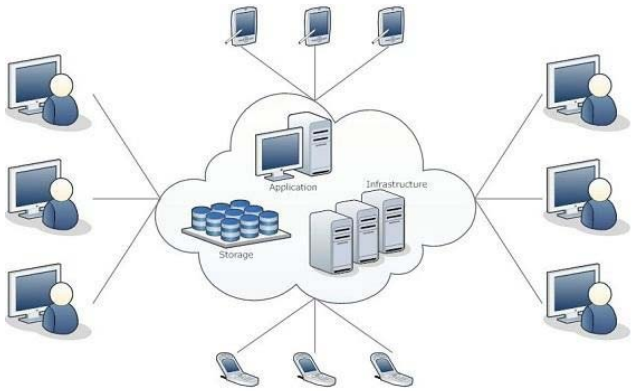

Figure 1. Cloud Computing [3]

To take advantages of cloud computing we must install some software on our local machine and that's it, this is the reason that makes cloud computing platform independent.

A. *Types of Cloud Computing:*

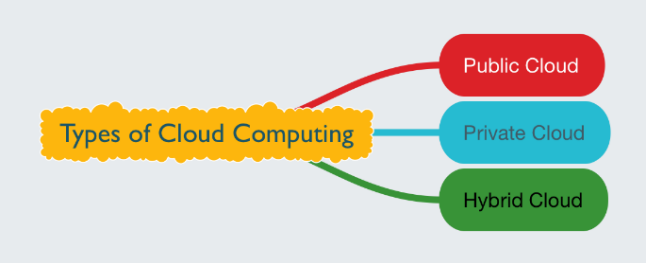

Figure 2. Types of Cloud Computing

Public Cloud: The public cloud makes it easy to access cloud services to the public. The examples of public cloud are Amazon, Microsoft, Dropbox, IBM, Rackspace, Google etc.

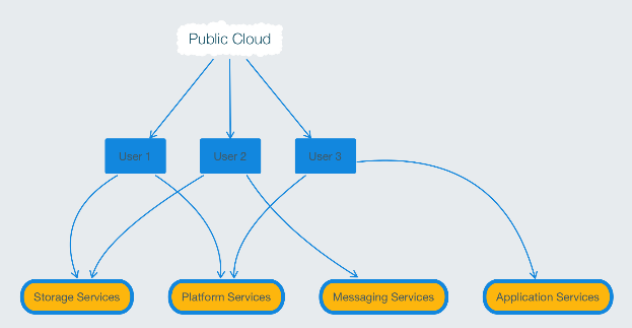

Figure 3. Public Cloud

Private Cloud: The Private cloud is accessible only within an organization or company, it is more secure than public cloud due to its limitations and restrictions. It will operatewithinan organization but can be managed by the third party [5].

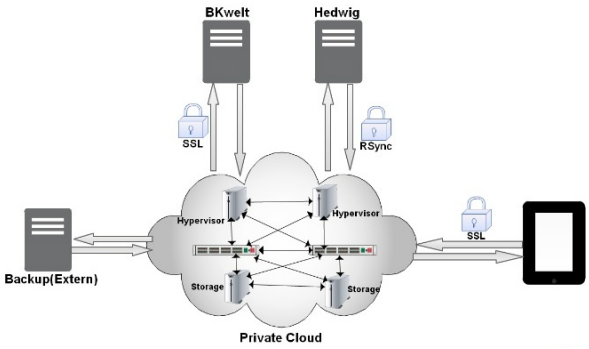

Figure 3. Private Cloud [6].

Hybrid Cloud: It is a combination of Public Cloud and Private Cloud, it is establishing a link between public cloud and private cloud.

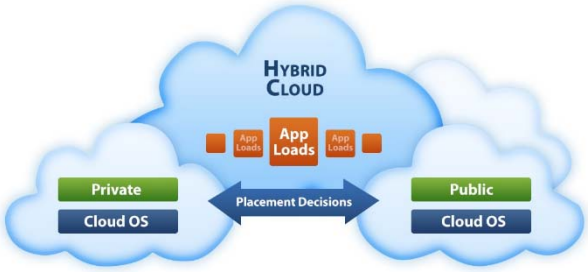

Figure 4. Private Cloud [7].

B. *Cloud Service Models:*

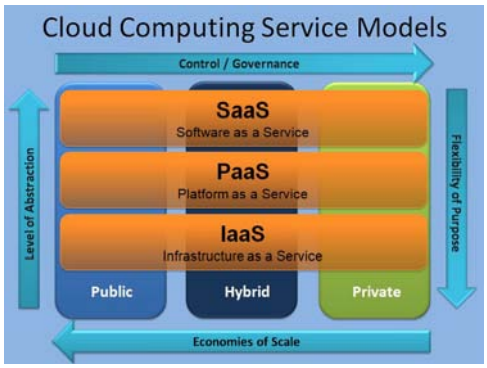

Figure 5. Cloud Computing Service Model [8]

Software as a Service (SaaS): In Software as a Service (SaaS), Cloud providers provide the software through the cloud, in other words, they manage the software in the cloud and user access the software through the cloud clients. Usually, cloud sources are hidden to the users, the usermust install the software on his own machine, rest of the works will be done in thecloud.Google Apps, Salesforce, Workday, Concur, Citrix GoToMeeting, Cisco WebEx are the examples of SaaS [9].

Platform as a Service (PaaS): PaaS provides a platform, a computing platform, in which they provide an operating system, a programming language, web servers, database etc. so that programmer can develop and run their applications directly in the cloud at minimum cost without purchasing extra

hardware or software. AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos are the example of PaaS[8][10].

Infrastructure as a Service (IaaS): It is a self-service model, it is providing entire hardware solution via the cloud, such as storage, networking, servers, processors, virtual machines and other components. Customer access all these services through internet and pay as per usage. Amazon EC2, Windows Azure, Rackspace, Google Compute Engine are the example of Infrastructure as a Service [9] [11].

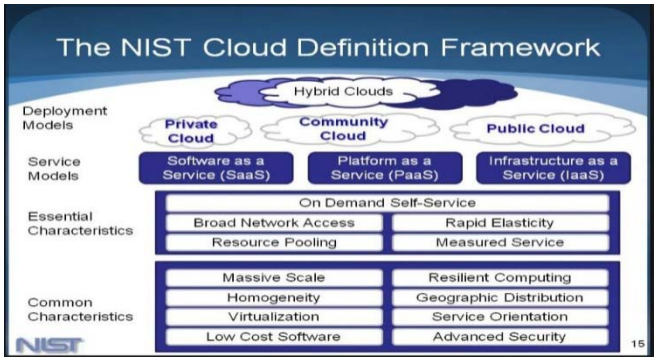

Figure 6. NIST Cloud Model [2].

IV. SECURITY CHALLENGES IN CLOUD COMPUTING

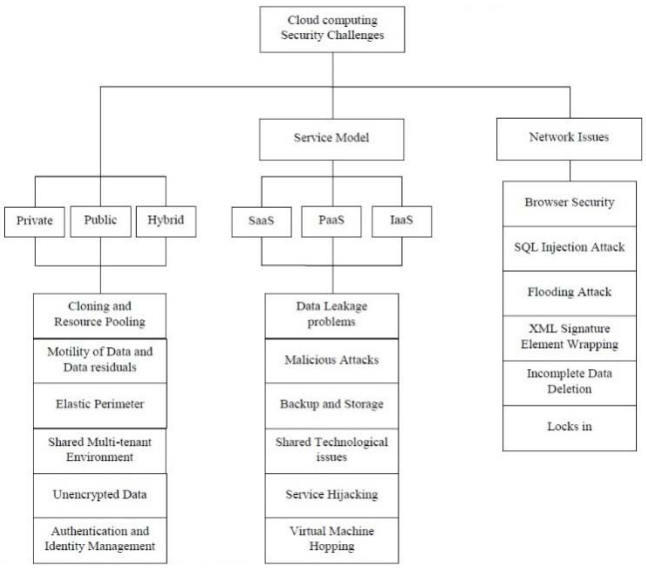

Figure 7. Classification of Security Challenges [18]

In 2013 Cloud Security Alliance (CSA) did a survey on cloud computing and identified top nine security threats in the cloud and named it "The Notorious Nine", in order to their severity these critical challenges are: 1. Data Breaches, 2. Data Loss, 3. Traffic Hijacking, 4. Insecure APIs, 5. Denial of Service, 6. Malicious Insiders, 7. Abuse of Cloud Services, 8. Shared Technology Issues, 9. Due diligence [2].

A. *Data Breaches*

When an unauthorized person or group of people enter in protected, secure, sensitive or confidential data then data breach occurs. Usually, attacker's target is not the user but ultimately user also gats affected. Here are some examples of data breaches: 1. Sony's PlayStation Network, in April 20, 2011, 77 million accounts hacked of PlayStation Network, according to Sony! The site was down for one month and they had lost million [12]. 2. Dropbox, in 2012 68 million accounts hacked [13]. 3. Evernote, in 2013 more than 50 million accounts hacked of Evernote [14]. 4. LinkedIn, in 2012 165 million accounts hacked [15]. There are many other examples also of data breaches attacks like yahoo!, Tumbler etc.

B. *Data Loss*

There are some reasons for data loss, the first reason ismalicious attacks, the second one is natural disasters, the third one is accidental deletion by the cloud service provider, the fourth one is a physical catastrophe. The malicious attacks are some hacker break the security wall of the account and then enter then delete all the data stored in it. The natural disasters are anearthquake, flood etc., the physical catastrophe like fire. All these things can have lost the customer's data forever unless cloud service provider takes proper backup of data [16].

C. *Account or Service Hijacking*

Phishing, fraud, and software exploitation vulnerabilities are the major attacks methods to hijack any account and they still achieve results, credentials, and passwords can be reused, which augment the impact of such attacks. All the transactions achieve network traffic between user and cloud service provider. When an assailant gains entry to a user's credentials, then he eavesdrops on the user's transactions and personal details [2] [16].

D. *Insecure APIs*

Orchestration, monitoring and cloud management interfaces are the very basic architecture of cloud computing, API or Application Programming Interface is the elemental component of availability and security in the services of cloud, and it is determining how different software chunks should collaborate with each other, so a fragile interface can be a deliberated threat to the Confidentiality, Integrity, and Availability of the data which is stored in the cloud [2].

E. *Denial-Of-Service*

The very basic definition of Denial-Of-Service is user is not able to access their data or their applications from the cloud as attackers prevent the user to access it, they are doing it by forcing victim cloud service provider to consume more processing power, reducing network bandwidth or memory space, it causes painful system slowdown and make user angry to the cloud service provider, because user understands that it is happening due to cloud service provider's bad service [16].

F. *Malicious Insiders*

This type of threatsis the most dangerous one, because insiders are involved in this type of attacks, usually insiders are the one who knows about the company more than outsiders attackers, that's why they are more harmful, because they know the weakness of the company and some other sensitive and confidential information, mostly they are the current or former employees of the company who has authorization on the company's network system [16].

G. *Abuse of Cloud Services*

Cloud Computing is known for providing virtual hardware at very low cost, even a small organization can work with vast amount of computing power with the help of cloud computing, rather than they purchase expensive computer component, but sometimes this cloud computing benefit become a threat for cloud computing itself, because attacker can't do much with his limited hardware but he can do a lot of harmful things with thousands of servers that virtually provided by the cloud service provider at very minimum cost [16].

H. *Insufficient Due Diligence*

According to ISO 37500 due diligence is "*detailed assessment of one or more business processes or production lines, culture, assets, liabilities, intellectual property, judicial and financial situation in order to make an acquisition or obtain accountability*" [17].

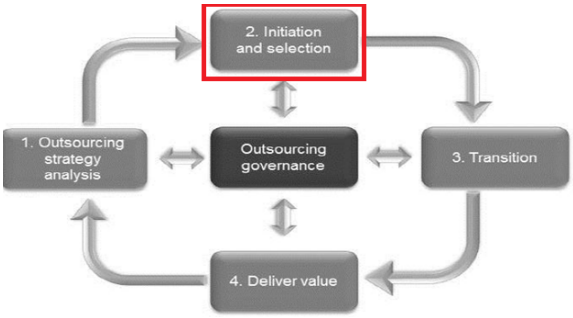

Figure 7. Due Diligence [17].

I. *Shared Technology Vulnerabilities*

Cloud Service Providers distribute their services in anextensible fashion bysharing applications,infrastructure, and platforms. Whether it's the elementalfactor that makes up this infrastructure that was not designed to offer strong segregation properties for Infrastructure as a Service (IaaS), Platforms as a Service (PaaS), or Software as a Service (SaaS), the threat of shared vulnerabilities exists in all delivery models. According to CLOUD SECURITY ALLIANCE. The Notorious Nine: Cloud Computing Top Threats in 2013 (pdf)"*A defensive in-depth strategy is recommended and should include computer, storage, network, application and user security enforcement, and monitoring, whether the service model is IaaS, PaaS, or SaaS. The key is that a single vulnerability or misconfiguration can lead to a compromise across an entire provider's cloud*" [16].

V. CONCLUSION

Despite that cloud computing is the best solution for storage and virtual hardware, it still has serious security concerns that can fail any organization at any time. In this paper, we have discussed cloud computing and its features, some major security issues that are needed to be solved. The only weakness of cloud computing is its security challenges, if somehow security challenges could be solved in the future then cloud technology and its providers can gain more consumers.

VI. REFERENCES

[1] Napoleon c. Paxton, member, ieee, "cloud security: a review of current issues and proposed solutions", 2016 ieee 2nd international conference on collaboration and internet computing.

[2] Priya anand, jungwoo ryoo, hyoungshick kim "addressing security challenges in cloud computing – a pattern-based approach", 2015 first international conference on software security and assurance, 978-1-5090-1078-3/16 $31.00 © 2016 ieee, doi 10.1109/icssa.2015.1113

[3] Https://www.tutorialspoint.com/cloud_computing/cloud_computing_overview.htm, tutorialspoint, cloud computing overview, retrieved date: 11/04/2017

[4] Https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/, azure.microsoft.com, what is cloud computing?, retrieved date: 11/04/2017

[5] Https://www.javatpoint.com/private-cloudjavatpoint, private cloud, retrieved date: 19/04/2017

[6] Https://creately.com/diagram/example/ha10lk2e1/private%20cloud%20diagram, creately.com, retrieved date: 19/04/2017].

[7] Http://www.webhostingsearch.com/articles/hybrid-cloud-hosting-in-depth, whs, when to use hybrid cloud hosting, retrieved date: 19/04/2017

[8] Http://cloudcomputingnet.com/cloud-computing-models/,cloud computing net, cloud computing models, retrieved date: 19/04/2017

[9] Https://apprenda.com/library/paas/iaas-paas-saas-explained-compared/, apprenda, iaas, paas, saas (explained and compared), retrieved date: 19/04/2017

[10] Http://stackoverflow.com/questions/16820336/what-is-saas-paas-and-iaas-with-examples, stackoverflow, what is saas, paas and iaas? With examples, retrieved date: 19/04/2017

[11] Https://www.javatpoint.com/infrastructure-as-a-service, javatpoint, infrastructure as a service | iaas, retrieved date: 19/04/2017

[12] Http://www.csoonline.com/article/2130877/data-protection/data-protection-the-15-worst-data-security-breaches-of-the-21st-century.html?page=2 cso online, the 15 worst data security breaches of the 21st century, retrieved date: 20/04/2017

[13] Http://www.tomsguide.com/us/pictures-story/872-worst-data-breaches.html#s13 toms guide, the worst data breaches of all time, by elizabeth palermo & paul wagenseil dec 14, 2016, 4:15 pm, retrieved date: 20/04/2017

[14] Http://www.tomsguide.com/us/pictures-story/872-worst-data-breaches.html#s17, toms guide, the worst data breaches of all time, by elizabeth palermo & paul wagenseil dec 14, 2016, 4:15 pm, retrieved date: 20/04/2017

[15] Http://www.tomsguide.com/us/pictures-story/872-worst-data-breaches.html#s6, toms guide, the worst data breaches of all time, by elizabeth palermo & paul wagenseil dec 14, 2016, 4:15 pm, retrieved date: 20/04/2017

[16] Top threats working group the notorious nine cloud computing top threats in 2013, by co-chairs (rafal los, hp dave shackleford, voodoo security bryan sullivan, microsoft), csa global staff (alex ginsburg, copywriter luciano jr santos, research director evan scoboria, webmaster kendall scoboria, graphic designer john yeoh, research analyst).

[17] Http://blog.itil.org/2015/01/kategorie-liste-home/itil/cloud-service-vendor-evaluation-and-due-diligence/, blog.itil, cloud service vendor evaluation and due diligence, by ben martin, published date: 28/01/2015, retrieved date: 20/04/2017

[18] Ms. Disha h. Parekh, dr. R. Sridaran, an analysis of security challenges in cloud computing, (ijacsa) international journal of advanced computer science and applications, vol. 4, no.1, 2013

[19] Khalid ei makkaoui*, abdellah ezzati, abderrahim beni-hssane, cloud security and privacy model for providing secure cloud services, 978-1-4673-8894-8/16/$31.00 ©2016 ieee.

[20] Rabi prasad padhy, manas ranjan patra, suresh chandra satapathy, "cloud computing: security issues and research challenges", iracst - international journal of computer science and information technology & security (ijcsits)vol. 1, no. 2, december2011